(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
25 octobre 2001 (25.10.2001)

PCT

(10) Numéro de publication internationale
WO 01/80563 A1

(51) Classification internationale des brevets[7] : H04N 7/16, 5/00

(21) Numéro de la demande internationale :
PCT/IB01/00604

(22) Date de dépôt international : 11 avril 2001 (11.04.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :

00810331.9	17 avril 2000 (17.04.2000)	EP
1179/00	15 juin 2000 (15.06.2000)	CH

(71) Déposant *(pour tous les États désignés sauf US)* : NAGRAVISION S.A. [CH/CH]; 22, route de Genève, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : STRANSKY, Philippe [CH/CH]; Pré-Fontaine H, CH-1261 Marchissy (CH).

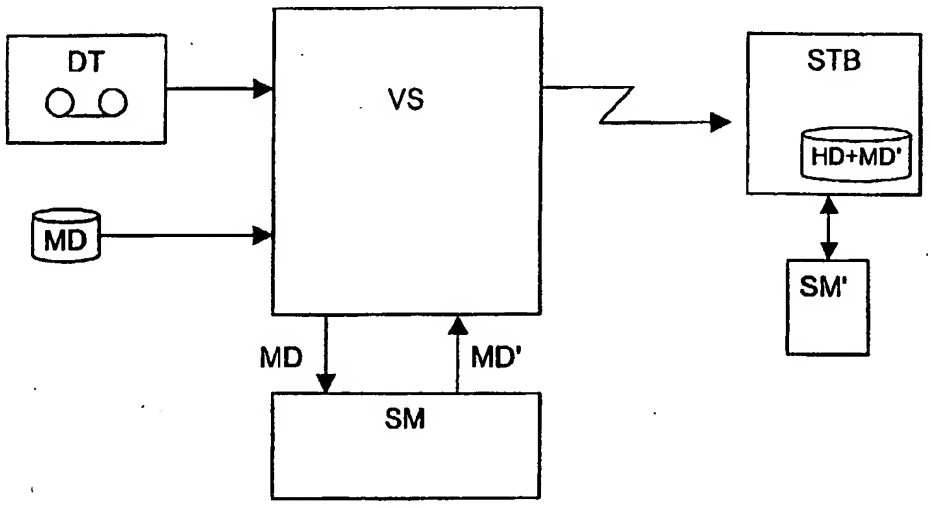
(74) Mandataire : LEMAN CONSULTING S.A.; 62, route de Clementy, CH-1260 Nyon (CH).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO,

[Suite sur la page suivante]

(54) Title: SECURE DATA TRANSMISSION SYSTEM AND METHOD

(54) Titre : SYSTEME ET METHODE DE TRANSMISSION SECURISE DE DONNEES



(57) Abstract: The invention concerns a system and a method for transmitting and storing audio/video data in encrypted form between a broadcasting centre and at least a processing module. Instead of transmitting data enabling decryption parallel to said data, said data are assembled in a decryption data file also comprising data defining access conditions to said audio/video data. Said file is stored independently of said data for immediate use or for deferred use.

(57) Abrégé : Cette invention concerne un système et une méthode de transmission et de stockage de données audio/vidéo sous forme encryptées entre un centre de diffusion et au moins un module d'exploitation. Au lieu de transmettre les informations permettant le décryptage parallèlement auxdites données, ces informations sont regroupées dans un fichier de données de décryptage comprenant également des données définissant les conditions d'accès auxdites données audio/vidéo. Ce fichier est stocké indépendamment desdites données et peut servir soit immédiatement ou soit lors d'une utilisation différée.

WO 01/80563 A1

NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

SYSTEME ET METHODE DE TRANSMISSION SECURISE DE DONNEES

Cette invention est du domaine de la sécurisation de données, en particulier la sécurisation de données lors du transport.

Dans un schéma classique de distribution, le générateur des données, que celles-ci soient des informations audio/vidéo ou un programme informatique, les transmet à un diffuseur qui est en charge de les distribuer contre payement.

Selon ce schéma connu, les données sont donc stockées en clair chez le distributeur, ce dernier possédant des moyens d'encryptage lors de la diffusion au consommateur final.

Les données sont usuellement acheminées depuis le fournisseur jusqu'au diffuseur par un moyen tel qu'une liaison câblée ou par l'envoi d'un support de données, par exemple une bande magnétique.

Il a été constaté que ce transport présente un risque important de copies illicites, les données en clair se prêtant aisément à la copie.

Forts de cette constatation, fournisseur et diffuseur se sont mis d'accord pour que le transport de ces données de fasse uniquement après l'encryptage desdites données.

Cette solution est satisfaisante du point de vue d'un détournement illicite de ces données lors du transport. Une fois les données arrivées à bon port, elles sont lues et stockées sur un serveur vidéo en vue de leur diffusion.

Néanmoins, le fournisseur, une fois les données transmises au diffuseur, perd le contrôle sur ses données et des copies illicites peuvent être produites à partir du serveur vidéo par des personnes mal intentionnées.

Ce même problème se retrouve lorsque le diffuseur transmet ces données encryptées au consommateur final qui a donc les moyens de les décrypter et peut ainsi en disposer en clair. Des copies non autorisées peuvent alors être produites depuis ce consommateur.

De plus, l'apparition de normes d'encryption dans le domaine de transmission de données limite les possibilités de sécurisation en imposant les algorithmes utilisés.

Le but de la présente invention est d'assurer la diffusion de données au travers de tous les différents intermédiaires tout en assurant un contrôle sur le nombre d'utilisations de ces données.

Ce but est atteint par un système de transmission de données audio/vidéo sous forme encryptées par un premier type d'encryption, lesdites données encryptées étant accompagnées par un fichier de données de décryptage, comprenant les clefs de décryptage temporel et les informations d'accès conditionnel, ledit fichier étant encrypté par un deuxième type d'encryption.

Ainsi, l'unité en charge de décrypter les données audio/vidéo va, sur la base des informations d'accès conditionnel, déterminer si l'utilisateur possède les droits nécessaires.

L'utilisation d'un deuxième type d'encryption permet de renforcer une encryption basée sur un système connu car imposé par une norme.

Le système au niveau de l'abonné

Afin de rendre les transmissions de données inviolables, le flux transmis comprend les données encryptées par des mots de contrôle CW ainsi que des informations de décryptage contenues dans un fichier appelé MT (Meta Data). Les mots de contrôle (CW) jouent le jeu de clefs de décryptage variant dans le temps. Ce fichier de Meta Data contient d'une

part les clefs de décryptage sous la forme de mots de contrôle CW et d'autre part une définition des droits nécessaires au décryptage que ce soit un abonnement ou le payement d'une redevance directement liée à cette émission. Ce fichier est encrypté par un algorithme de type IDEA dont la sécurité est supérieure aux algorithmes utilisés pour l'encryption par mots de contrôle (CW).

Du côté de l'abonné se trouve un module de sécurité, usuellement sous la forme d'une carte à puce, qui contient les droits de l'abonné (son crédit entre autre) et compare ses droits avec ceux requis par l'émission. Si les droits le permettent, le module de sécurité décrypte le fichier de Meta Data et retourne les mots de contrôle CW nécessaires au décryptage des données.

De plus en plus d'installations d'abonnés comprennent des unités de stockage des informations tel qu'un disque dur. Ceci permet de revisualiser une scène, d'effectuer un ralenti tout en ne perdant nullement les informations diffusées pendant la revisualisation.

Ces unités sont capables de stocker l'entier d'un film pour le proposer ensuite à la vente à l'abonné. Un tel téléchargement se fait en général la journée, période pendant laquelle le trafic est le plus faible. Si l'abonné accepte la proposition d'achat, il peut le visualiser quand bon lui semble.

Ce procédé présente l'inconvénient de disposer sur un support numérique donc facilement copiable, d'informations dont on désire contrôler l'utilisation. Ceci est également valable lors de la transmission de logiciel. En effet, l'installation de l'abonné peut être un ordinateur sur lequel est connecté un module de sécurité et le téléchargement peut représenter une programme de jeu par exemple.

Selon l'invention, les données sont transmises encryptées par un premier type d'encryption, accompagnées par un fichier de messages de contrôle

étant eux-mêmes encryptés par une clé de distribution selon un deuxième type d'encryption. Dans ce fichier sont également inclus les informations d'accès conditionnel, définissant les droits à une utilisation immédiate et les droits associés à une utilisation différée.

Le flux de données est stocké sous forme encryptée dans l'unité de l'abonné, ceci interdisant toute utilisation abusive. Chaque utilisation subséquente des données nécessite la présence du module de sécurité. Ce dernier peut alors contrôler les droits d'une utilisation différée, par exemple pour la limiter dans le temps, voire de ne l'autoriser qu'un certain nombre de fois.

Dans le cas ou un certain nombre d'utilisation est autorisée, le message de contrôle comprend l'identificateur de l'émission, le nombre maximum d'utilisation ainsi qu'éventuellement un indicateur de persistance. Lors de la première utilisation, le module de sécurité va initialiser un compteur propre à cette émission qui sera incrémenté à chaque décryptage par le module de sécurité. Lorsque le maximum est atteint, le décryptage sera interdit.

L'indicateur de persistance permet au module de sécurité de savoir dans quel délai le compteur de cette émission peut être effacé. Afin de ne pas remplir la mémoire du module de sécurité avec ces informations, lorsque la date de cet indicateur est dépassée, la portion de mémoire allouée à cette opération peut être réutilisée. Il est avantageusement libellé en jour (1 à 250 jours) à partir de la première utilisation.

Le système au niveau du diffuseur

Le diffuseur dispose d'une gigantesque unité de stockage qui regroupe toutes les émissions à diffuser. On l'appelle couramment serveur vidéo. Certaines émissions seront diffusées une fois, telles que les informations

télévisées, alors que d'autres vont être diffusées en boucle pendant plusieurs jours afin d'être proposées à l'achat aux abonnés.

Ces émissions arrivent cryptées, accompagnées par des messages de contrôle cryptés par une première clé propre au fournisseur. Ces données sont stockées dans l'unité de stockage sous forme cryptée afin de prévenir toute fuite ou copie illicite.

Lors de l'utilisation de ces données, le serveur vidéo transmet les données encryptées en vue de leur diffusion. Ces données sont accompagnées par l'envoi par le serveur vidéo, du fichier des informations de décryptage à une unité de sécurité.

Cette unité effectue un décryptage de ce fichier afin d'en extraire les mots de contrôle CW et de vérifier les droits d'utilisation. Une fois cette opération terminée, le module de sécurité encrypte ces mots de contrôle en y joignant de nouveaux droits d'utilisation. Ces nouveaux droits sont définis par le diffuseur et peuvent comprendre une condition sur un abonnement ou lier l'utilisation à l'achat de l'émission. C'est à ce stade que le nombre d'utilisation, soit de visualisation, est défini.

Ce nouveau fichier d'informations de décryptage est ensuite transmis avec le flux de données encryptées.

L'invention sera mieux comprise grâce à la description détaillée qui va suivre et qui se réfère aux dessins annexés qui sont donnés à titre d'exemple nullement limitatif, dans lesquels les figures 1 et 2 représentent deux variantes de l'invention.

Le serveur vidéo VS reçoit les données DATA sous forme de bande selon notre exemple mais qui peuvent être transmises par n'importe quel moyen connu de transmission. Le fichier des informations de décryptage MD est également fourni au serveur vidéo. Ce fichier est généralement fourni en même temps c'est-à-dire qu'il se trouvera avantageusement sur la même

bande que les données encryptées. Néanmoins, si l'on désire renforcer la sécurité, il est possible de faire transiter le fichier MD par d'autres moyens.

Une fois ces deux fichiers dans le serveur vidéo VS, le système est prêt pour la diffusion.

A ce moment, le fichier MD est transmis au module de sécurité SM pour y adjoindre les droits que l'on désire définir pour cette émission. Le module décrypte le fichier MD puis ajoute les informations relatives aux droits nécessaires à la visualisation et retourne au serveur VS ce nouveau fichier MD' encrypté par une clef de transport.

Les données DT ainsi que ce nouveau fichier sont diffusés à l'intention des différents modules d'abonné STB.

Du fait que le décryptage des données DT ne peut se faire sans le fichier MD', celui-ci est en général envoyé préalablement.

Les données arrivant au décodeur STB sont soit traitées immédiatement, soit stockées pour usage ultérieur dans l'unité HD. Dans ce deuxième cas, il est clair que le fichier MD' doit également être stocké dans l'unité HD tel qu'illustré à la figure 1.

Pour obtenir les données en clair, ce fichier MD' est présenté au module de sécurité de l'abonné SM' afin qu'il puisse décrypter ledit fichier et en extraire les mots de contrôle CW.

Selon une variante de l'invention telle qu'illustrée dans la figure 2, le fichier MD' est stocké uniquement dans le module de sécurité de l'abonné SM'. Ainsi, toute tentative de rechercher les corrélations entre le contenu des données et le fichier MD', est vouée à l'échec.

Dans le cadre de l'invention, il est proposé un module de pré-encryptage destiné à produire les données DT sous forme encryptées. Ce module

reçoit les données en clair et produit le couple de données encryptées DT et le fichier MD.

Selon la structure de sécurité choisie, le fichier DT est encrypté selon un premier mode d'encryption, les mots de contrôle CW servant de clés de décryption. Il s'agit de préférence d'un mode symétrique du fait de la rapidité exigée pour le traitement. Ces mots de contrôle CW sont à leur tour encryptés selon un deuxième mode d'encryption, DES par exemple.

Lorsqu'il s'agit de grouper l'ensemble des mots de contrôle dans un fichier MD, l'encryption de ce fichier est d'un troisième type de haut niveau cryptographique, par exemple IDEA. En effet, les conséquences d'une attaque victorieuse sur ce fichier étant bien plus grave que sur un mot de contrôle.

REVENDICATIONS

1. Système de transmission et de stockage de données audio/vidéo sous forme encryptées entre un centre de diffusion et au moins un module d'exploitation, caractérisé en ce qu'un fichier de données de décryptage comprenant les clefs de décryptage temporel et des données définissant les conditions d'accès aux dites données audio/vidéo sont transmises et stockées parallèlement aux dites données audio/vidéo.

2. Système selon la revendication 1, caractérisé en ce que les données définissant les conditions d'accès comprennent au moins une section définissant les droits d'utilisation immédiate des données audio/vidéo et une section définissant les droits d'utilisation différée desdites données audio/vidéo.

3. Système selon la revendication 2, caractérisé en ce que la section définissant les droits d'utilisation différée comprend le type d'abonnement nécessaire, le prix de l'utilisation des données ou le nombre d'utilisation maximum.

4. Système selon les revendications 1 à 3, caractérisé en ce que le module d'exploitation est un récepteur de vidéo à péage (STB) muni d'un module de sécurité (SM') et que les données audio/vidéo sont reçues et stockées dans une unité de stockage (HD).

5. Système selon la revendication 4, caractérisé en ce que les données définissant les conditions d'accès sont stockés dans le module de sécurité (SM').

6. Système selon les revendications 3 et 4, caractérisé en ce que le module de sécurité comprend une mémoire dans laquelle est inscrit une référence et le nombre d'utilisation desdites données audio/vidéo.

7. Système selon les revendications 1 à 3, caractérisé en ce que le module d'exploitation est un serveur vidéo (VS) disposant d'un module de sécurité (SM) en charge de définir les données définissant les conditions d'accès aux dites données audio/vidéo.

8. Méthode de transmission et de stockage de données audio/vidéo sous forme encryptées entre un centre de diffusion et au moins un module d'exploitation comprenant les étapes suivantes:

- encryptage de données audio/vidéo au moyen de clefs de cryptage (CW) variant en fonction du temps
- encryptage d'un fichier (MT) formé par les clefs de cryptage et les conditions d'accès aux dites données audio/vidéo
- transmission et stockage des données audio/vidéo indépendamment du fichier (MT).

9. Méthode selon la revendication 8, caractérisée en ce que le module d'exploitation est un récepteur de vidéo à péage (STB) muni d'un module de sécurité (SM') et qu'elle consiste à recevoir et stocker les données audio/vidéo dans une unité de stockage (HD).

10. Méthode selon la revendication 9, caractérisée en ce qu'elle consiste à stocker les données définissant les conditions d'accès dans un module de sécurité (SM') connecté au récepteur (STB).

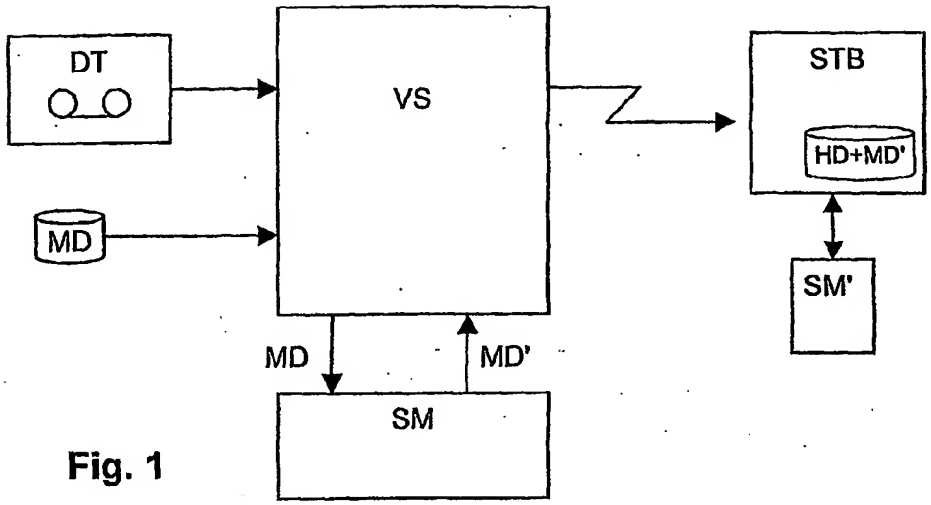


Fig. 1

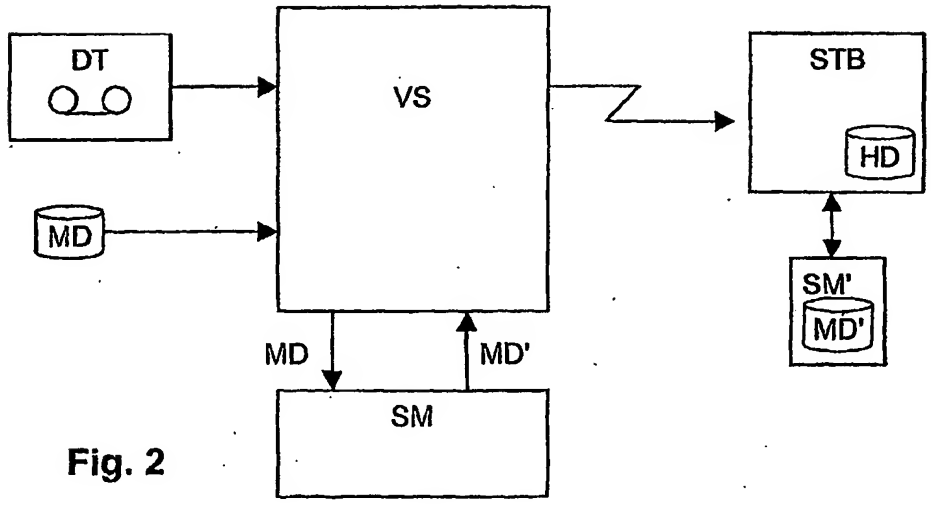


Fig. 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 01/00604

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16 H04N5/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 46017 A (THOMSON CONSUMER ELECTRONICS) 4 December 1997 (1997-12-04) page 4, line 8 -page 10, line 30 page 14, line 17 -page 16, line 12 page 19, line 6 -page 21, line 31 figures 1-4	1-6,8-10
X	EP 0 715 241 A (MITSUBISHI CORP) 5 June 1996 (1996-06-05)	1,7-10
Y	page 7, column 12, line 48 -page 9, column 15, line 41 page 15, column 28, line 1 -column 16, line 54 figures 3-5,8,14	2-6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 July 2001	17/07/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Van der Zaal, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 01/00604

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 975 165 A (SONY CORP) 26 January 2000 (2000-01-26) page 3, column 4, line 6 -page 5, column 7, line 11 page 5, column 8, line 10 -page 6, column 10, line 19 -----	2-6

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 01/00604

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9746017 A	04-12-1997	US 5933500 A	03-08-1999
		AU 3150797 A	05-01-1998
		AU 3150897 A	05-01-1998
		AU 3209497 A	05-01-1998
		AU 716349 B	24-02-2000
		AU 3213297 A	05-01-1998
		AU 3213397 A	05-01-1998
		BR 9709409 A	10-08-1999
		BR 9709410 A	10-08-1999
		BR 9709420 A	10-08-1999
		BR 9709494 A	10-08-1999
		BR 9709508 A	10-08-1999
		CN 1226354 A	18-08-1999
		CN 1226359 A	18-08-1999
		CN 1226355 A	18-08-1999
		CN 1226356 A	18-08-1999
		CN 1226357 A	18-08-1999
		EP 0903033 A	24-03-1999
		EP 0903034 A	24-03-1999
		EP 0903035 A	24-03-1999
		EP 0903036 A	24-03-1999
		EP 0903038 A	24-03-1999
		JP 2000511019 T	22-08-2000
		JP 2000511020 T	22-08-2000
		JP 2001502854 T	27-02-2001
		JP 2000512095 T	12-09-2000
		PL 330219 A	10-05-1999
		TR 9802484 T	22-03-1999
		WO 9746007 A	04-12-1997
		WO 9746008 A	04-12-1997
		WO 9746009 A	04-12-1997
		WO 9746010 A	04-12-1997
		US 5844595 A	01-12-1998
		US 5838873 A	17-11-1998
		US 5844478 A	01-12-1998
		US 5754651 A	19-05-1998
EP 0715241 A	05-06-1996	JP 8287014 A	01-11-1996
		US 5867579 A	02-02-1999
		US 6128605 A	03-10-2000
EP 0975165 A	26-01-2000	CN 1115150 A	17-01-1996
		EP 0691787 A	10-01-1996
		JP 8077706 A	22-03-1996
		US 5796828 A	18-08-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/IB 01/00604

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/16 H04N5/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 97 46017 A (THOMSON CONSUMER ELECTRONICS) 4 décembre 1997 (1997-12-04) page 4, ligne 8 -page 10, ligne 30 page 14, ligne 17 -page 16, ligne 12 page 19, ligne 6 -page 21, ligne 31 figures 1-4	1-6,8-10
X	EP 0 715 241 A (MITSUBISHI CORP) 5 juin 1996 (1996-06-05)	1,7-10
Y	page 7, colonne 12, ligne 48 -page 9, colonne 15, ligne 41 page 15, colonne 28, ligne 1 -colonne 16, ligne 54 figures 3-5,8,14	2-6

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
10 juillet 2001	17/07/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Van der Zaal, R

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

inde Internationale No
PCT/IB 01/00604

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
Y	EP 0 975 165 A (SONY CORP) 26 janvier 2000 (2000-01-26) page 3, colonne 4, ligne 6 -page 5, colonne 7, ligne 11 page 5, colonne 8, ligne 10 -page 6, colonne 10, ligne 19	2-6

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/IB 01/00604

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9746017 A	04-12-1997	US 5933500 A	03-08-1999
		AU 3150797 A	05-01-1998
		AU 3150897 A	05-01-1998
		AU 3209497 A	05-01-1998
		AU 716349 B	24-02-2000
		AU 3213297 A	05-01-1998
		AU 3213397 A	05-01-1998
		BR 9709409 A	10-08-1999
		BR 9709410 A	10-08-1999
		BR 9709420 A	10-08-1999
		BR 9709494 A	10-08-1999
		BR 9709508 A	10-08-1999
		CN 1226354 A	18-08-1999
		CN 1226359 A	18-08-1999
		CN 1226355 A	18-08-1999
		CN 1226356 A	18-08-1999
		CN 1226357 A	18-08-1999
		EP 0903033 A	24-03-1999
		EP 0903034 A	24-03-1999
		EP 0903035 A	24-03-1999
		EP 0903036 A	24-03-1999
		EP 0903038 A	24-03-1999
		JP 2000511019 T	22-08-2000
		JP 2000511020 T	22-08-2000
		JP 2001502854 T	27-02-2001
		JP 2000512095 T	12-09-2000
		PL 330219 A	10-05-1999
		TR 9802484 T	22-03-1999
		WO 9746007 A	04-12-1997
		WO 9746008 A	04-12-1997
		WO 9746009 A	04-12-1997
		WO 9746010 A	04-12-1997
		US 5844595 A	01-12-1998
		US 5838873 A	17-11-1998
		US 5844478 A	01-12-1998
		US 5754651 A	19-05-1998
EP 0715241 A	05-06-1996	JP 8287014 A	01-11-1996
		US 5867579 A	02-02-1999
		US 6128605 A	03-10-2000
EP 0975165 A	26-01-2000	CN 1115150 A	17-01-1996
		EP 0691787 A	10-01-1996
		JP 8077706 A	22-03-1996
		US 5796828 A	18-08-1998